IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1-12. (Canceled).

13. (New) A user identification information protection method comprising the steps of:

performing a hierarchical encryption of a message containing an identification message of a mobile user by encrypting a part containing identification information of the mobile user in the message using an encryption key which is derived from subscription information of the mobile user, and by further encrypting the encrypted message using a public key of a home domain server;

routing the encrypted message to a network to which the home domain server belongs, using home domain information;

further concealing actual identification information of the mobile user using a temporary domain specific identifier; and

performing mutual authentication of a mobile terminal and a plurality of network elements using a challenge message response exchange scheme.

14. (New) The user identification information protection method according to claim 13, further comprising the steps of:

transmitting to an access point mobile terminal accesses, in the mobile terminal, the encrypted identification information of the mobile user, a challenge message for the access point, a challenge message for the network and the home domain information of the mobile user;

transmitting to a home domain server of the mobile user, in the access point, the encrypted identification information of the mobile user and the challenge message for the network, using the home domain information of the mobile user;

receiving from the home domain server of the mobile user, in the access point, an access point response key, a challenge message response for a home domain server of the access point and a challenge message response for the home domain server of the mobile terminal; and

receiving from the access point, in the mobile terminal, the challenge message response for the access point and the challenge message response for the home domain server of the mobile terminal transferred by the access point.

15. (New) The user identification information protection method according to claim 14, further comprising the step of:

in the step of transmitting the messages from the mobile terminal to the access point, encrypting the challenge message for the access point using a public key of the access point and encrypting the challenge message for the network using a public key of the home domain server.

16. (New) The user identification information protection method according to claim 14, further comprising the steps of:

transmitting from the mobile terminal to a central server, in the home domain server of the mobile user, a message comprising the challenge message for the network transferred by the access point; and

receiving, in the home domain server of the mobile user, the message comprising the access point response key transferred from the central server to the access point, the challenge message response for the access point and the challenge message response for the network of the mobile terminal.

17. (New) A mobile terminal comprising:

an encrypting section that performs a hierarchical encryption of a message containing identification information of a mobile user by encrypting a part containing the identification information of the mobile user in the message using an encryption key which is derived from subscription information of the mobile user, and by further encrypting the encrypted message using a public key of a home domain server;

a transmitting section that transmits to an access point mobile terminal accesses, in the mobile terminal, the encrypted identification information of the mobile user, a challenge message for the access point, a challenge message for the network and home domain information of the mobile user; and

a receiving section that receives from the access point, in the mobile terminal, a challenge message response for the access point and a challenge message response for the home domain server of the mobile terminal transferred by the access point.

18. (New) The mobile terminal according to claim 17, further comprising, in the transmitting section, a section that encrypts the challenge message for the access point using the public key of the access point and encrypts the challenge message for the network using a public key of the home domain server.

19. (New) An access point for mobile terminal accesses, comprising:

a receiving section that receives from a mobile terminal, encrypted identification information of a mobile user, a challenge message for the access point, a challenge message for a network and home domain information of the mobile user; and

a transmitting section that transmits the encrypted identification information of the mobile user and the challenge message for the network to a home domain server of the mobile user using the home domain information of the mobile user, wherein:

the receiving section further comprises a section that receives from the home domain server of the mobile user, an access point response key, a challenge message response for a home domain server of the access point, and a challenge message response for a home domain server of the mobile terminal; and

the transmitting section further comprises a section that transmits to the mobile terminal, the challenge message response for the access point and the challenge message response for the home domain server of the mobile terminal.